1. System requirements

In order to make encrypted phone calls, please make sure the data channel UMTS is enabled and configured for your SIM card (check with your telephone operator). Make sure you have a contract suitable for data transmission.

2. Starting the application

The Cryptech application starts automatically along with the device. The Cryptech home screen will appear on the display. If the application is idle for too long, it will be sent to the background by the Windows Mobile Operating System (i.e. you will not be able to see the application home screen on the device). To reactivate, simply select "Menu" from the Windows Mobile Home Screen and click on the Cryptech icon which appears on the display.

3. VoIP account setup

To connect to the VoIP network and be available you will first have to set the username (usually the phone number with country code) and the password for your account. To do this, simply press Menu > VoIP> Settings. If you use Cryptech 3G rarely or only at certain times of the day and for the remaining time you do not wish to be available, we recommend to remove the tick from "Connect at startup", also if you do not want the system to automatically connect when you start your phone, consuming battery and data traffic.

4. Voip server connection

To be able to call or be reachable in crypto mode, Cryptech 3G must be connected to the VoIP server. If the system is set to "Connect at startup", when the phone starts a data connection will be automatically set up and green VOIP text will be printed on the status bar of the Cryptech 3G home screen. If the VOIP text is coloured gray, it means that the application is disconnected or the connection is disabled at startup, in which case press Menu > Voip > Connect. If there is no VOIP text but three green dots appear in its place, it means that the system is trying to connect. If the three green dots persist for too long, usually it means that there is a problem with the connection (check the network configuration or the remaining billed data traffic). The connection with the VoIP server is only used to let users reach each other, whilst the encryption is always performed between the phones themselves.

5. Data traffic consumption

During encrypted voice communication, about 2.5 KB/s per second are consumed in UMTS/WiFi and about 1.3 KB/s over GPRS /EDGE coverage. When Cryptech 3G is idle (i.e. not in voice communication) but connected to the server VoIP, the data consumption is approximately 1 KB per day. It is important to take seriously in consideration these parameters in order to underwrite a proper data contract so as not to run the risk of spending too much money for data transfers. We recommend to underwrite a flat rate data contract with your operator. Since the battery consumption may be affected by the use of Cryptech 3G even when idle, we suggest to connect to the VoIP server only when you need to communicate in crypto.

6. Making an encrypted call

To make an encrypted call, while on the Cryptech home screen simply dial the number directly on your keyboard or import the contact from the phonebook (select "Contact" and choose the desired contact among those of Outlook Mobile). Then press the green call button, after a brief synchronization phase, the call is active. During synchronization, you will see a progress bar. The encrypted call starts upon progress bar completion (the coloured bar gets to 100%). If the bar turns red it means that the system is making a data retransmission due to errors in the connection.
To change the volume during the call you can use the up / down arrows on the multifunction key. The volume can also be set for all calls by selecting Menu > Audio on Cryptech home screen.

7. Receiving encrypted calls

To answer an incoming encrypted call, just press the green button when you hear the ringing. After a few seconds during which the encryption key is generated, the progress bar gets completed and you can begin to talk safely.

8. Automatic SMS Cryptech key generation

Cryptech by default generates automatically a cryptographic key for your SMS. When you make a crypto call to one of your contacts, at the beginning of the connection, Cryptech generates a specific key for that contact and will save it until the next call, when it will change it. You can see it on the display noticing that a green key will appear on the bottom of the screen.

9. UMTS,EDGE,GPRS,WIFI networks

Cryptech 3G è stato progettato per poter utilizzare qualunque rete di comunicazione internet disponibile sul telefono. E' importante configurare prima di tutto le impostazioni per la rete umts in modo che si possa essere sempre raggiungibili. Quando si è in vicinanza di router wifi (ad esempio in ufficio o in un hotspot pubblico) basta accendere sul telefono il wifi, configurare eventualmente la chiave di accesso, ed utilizzare Cryptech 3G su tale rete. In questo modo il traffico generato non influirà sulla bolletta telefonica. Si possono avere anche più connessioni attive (umts e wifi) in tal caso il telefono farà automaticamente passare il traffico sul wifi e tornerà ar utilizzare l'umts appena il wifi non è più disponibile. Cryptech 3G si può utilizzare anche in movimento ma in tal caso ci possono essere dei problemi di trasmissione relativi all' HANG OVER tra una cella e l'altra . questi problemi si manifestano come dei buchi nella comunicazione o dei ritardi nella trasmissione, che vengono recuperati non appena possibile. La qualità dell'audio e del ritardo si adattano continuamente ed in tempo reale in relazione alle prestazioni della rete. Se ci si trova in una zona con copertura GPRS o EDGE, la qualità sarà leggermente inferiore dovendosi adattare alla banda disponibile ed il ritardo sarà superiore per poter rendere la conversazione fluida nonostante l'irregolarità della trasmissione. In particolare il passaggio da una cella UMTS ad una GPRS e viceversa può generare un buco di diversi secondi.

Cryptech 3G is designed to use any communications network available on the internet phone. It's important to first configure the settings for UMTS network so that you can always be reached. When you are in the range of a WiFi router (e.g. office or public hotspot) just turn on the WiFi on the phone, configure the appropriate access key, and use Cryptech 3G services on the network. In this way the traffic will not affect your phone bill. You can also have more than one active connection (UMTS and WiFi), in this case the phone will automatically switch traffic between WiFi and UMTS depending on availability, trying firstly to connect via WiFi and switching to UMTS when the latter is no longer available. Cryptech 3G can also be used in motion but then there may be transmission problems relating to HANG OVER between the cells. These problems manifest as holes in the communication or transmission delays, which are recovered

Operations and Sales Office: Via Cardinal Massaia 83, 10147 Torino (TO), Italy
Tel.: +390112303634; Fax: +390112303632;
Web: http://www.caspertech.com; Email: info@caspertech.com

as soon as possible. The sound quality and delay continuously adapt in real time in relation to network performance. If you are in an area with EDGE or GPRS coverage, the quality will be slightly lower since the system will have to adapt to the available bandwidth and the delay will be higher in order to make the conversation flow linear despite the irregularity of the transmission. In particular the transition from one GPRS cell to a UMTS and vice versa can create an audio gap of several seconds.

10. User Authentication Password Setting

The user authentication password is used both to control access to the Cryptech application and to the storage area of the cryptographic keys which make your conversations secure. Per impostare la password di autenticazione utente selezionare dalla schermata Cryptech la voce Menu>Opzioni>Password Utente. Verrà richiesto di inserire la password due volte quindi cliccare su "Fatto". To set the user authentication password, from the Cryptech home screen select Menu > Options> User Password. You will be prompted for the password twice then click on "Done".

To set the password for user authentication screen, select Menu > Options > User Password. You will be prompted for the password twice then click on "Done."
Now you can set the device so that it will promt for a password at each book by selecting Menu> Options> Authentication Mode. In this window you can choose between "always" (password authentication will be asked each time you start Cryptech or device) and "never" (the password will not be required). In this section you can also enable / disable authentication on the encrypted call history and contacts.

> *Do not forget your authentication user password because without it Cryptech can't be launched and you will need to contact Casper Technology for software replacement/restore.*
>
> *For security reasons, we recommend not to enable Bluetooth® and GPRS connections (including those used to send/receive MMS). Also avoid installing or running applications other than those provided with the device.*
>
> *In order to keep the encryption software working, it's necessary never to perform the hard-reset operation which takes the phone back to its initial state and removes every application installed on the device.*

11. Static shared keys customization

Static cryptographic keys are shared by all the devices used to talk in encrypted mode with each other and are used to encrypt the whole conversation. They are often called "symmetrical" or "shared" because they must be identical for both interlocutors. Click "Menu", then "Options" and finally "Encryption Keys". Create at least one cryptographic key by selecting "New", then typing "1" in the "Priority level" field and your password in the field below.
To enter a key you can choose between text mode (default) and Hex mode. Most users can simply use the Text mode, type the encryption keys by using all available characters. Hex mode mode is included for users of a certain experience, and requires that the characters inserted as the encryption key are part of the hexadecimal encoding (0-9, A-F).
Notice that the keys chosen in this section are used to encrypt the conversations, whereas the user authentication password is used to grant access to Cryptech and to protect/manage the encryption keys storage. The value "1" means "highest priority" and is required in order to bypass the Cryptech test keys. Once you have successfully inserted your key/s, you can delete the Cryptech test keys with the "Delete Key" function: click on each key, select "Menu", then "Manage Key" and "Delete Key". Remember to set the same static shared keys on every device you want to communicate with, or consider using the Diffie-Hellman protocol to call in encrypted mode without sharing common keys.

12. Encrypted Contacts

Cryptech keeps you encrypted contacts apart from the normal phone book to facilitate crypto calls/messages and especially to protect the privacy of contacts. To access the contacts you need to enter the password for authentication. To create a contact number you can either type it by hand or import contacts from Microsoft on the phone. Alternatively, the system automatically creates the contact upon receiving or making encrypted calls with a contact. If you do not like the password authentication protecting your contacts, you can disable it by selecting Menu > Options> Authentication Mode.

13. Call History

Cryptech keeps track of calls made in crypto mode. Access to this list is password protected, which may be disabled if you wish. The list is encrypted to protect privacy.

14. Encryption modes management

The Cryptech application supports two types of encryption keys: static (shared) keys and dynamic (based on the Diffie-Hellman protocol) keys. Unlike static keys, the Diffie-Hellman protocol does not require user intervention: if you enable this feature, a dynamic key is created at the beginning of the call and deleted when this is terminated.

Both encryption with static shared keys and with dynamic keys guarantee absolute security, however in both cases there is a "human factor" to consider. Static keys must be shared by all interlocutors and, if their number is large, there is a certain risk that somebody inadvertedly discloses some keys. In the Diffie-Hellman protocol there is the remote possibility of an intruder messing with the dynamic key creation during the initial synchronization (this is called man-in-the-middle attack). Cryptech protects you from this risk by generating numerical authentication codes that appear on your screen during the call. Both interlocutors should communicate these codes to each other by voice: if they match, no intruder has interfered with the call. Since users may forget this additional protection, Cryptech can also use a combination of both static and dynamic keys that eliminates even the risk of "human negligence". However several options are available to provide maximum flexibility of usage.

By default Cryptech is pre-configured for highest security, i.e. combination of static and dynamic keys required. However the Security Levels can be managed (select Menu>Options>Security):

1. Shared Keys: You can select if a shared key can be optional or required. This way is possible to prevent communicating with Easy Cryptech devices that do not have shared keys or other Cryptech that do not have a key in common.
2. Diffie-Hellman: You can choose whether it will be optional, required or disabled. This way you can force the use of keys generated at the moment combined with static keys or exclude the use of Diffie-Hellman in order to have more control over the key used for encryption.
3. Diffie-Hellman protocol generates keys with calculations based on 571 bits elliptic curves (ECDH), if you remove the tick in this function, the system will use the standard Diffie-Hellman algorithm thus generating keys derived by 4096 bits prime numbers. In this case the generation is slower and less robust in security.
4. You can decide whether to generate automatically the encryption keys for SMS during a crypto call with the contact

15. Language Selection

Under Options > Language you will find the option to choose the language which will be used for the encryption software. By default, the same language as the Operating System is selected.

Operations and Sales Office: Via Cardinal Massaia 83, 10147 Torino (TO), Italy
Tel.: +390112303634; Fax: +390112303632;
Web: http://www.caspertech.com; Email: info@caspertech.com